

知 SecPath F5040(V7)在 ips配置文件中设置例外规则不记录日志不生效

IPS防攻击 会话 存储介质硬盘 王英凯 2019-05-28 发表

组网及说明

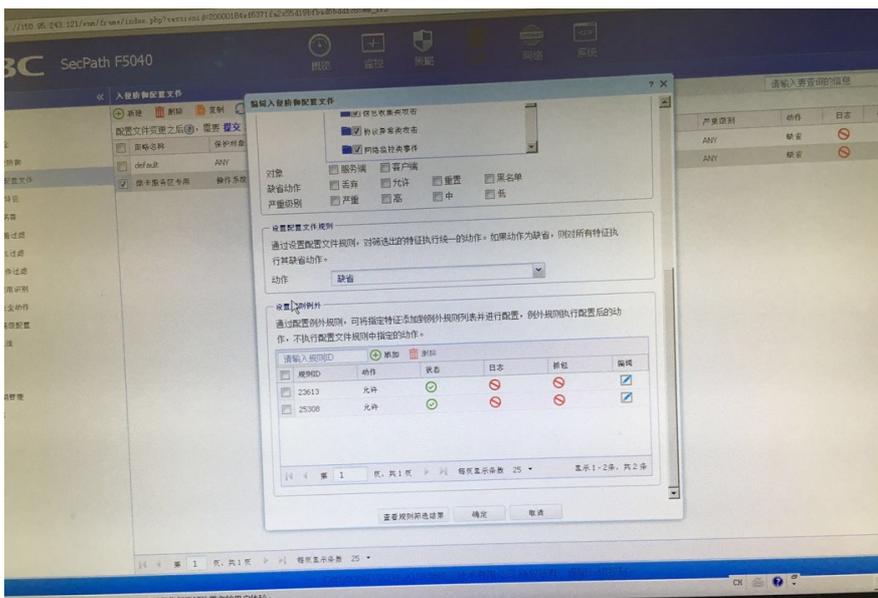
F5040做路由模式部署、配置IPS功能，特征库已经升级到官网最新版本，软件版本9320P25

问题描述

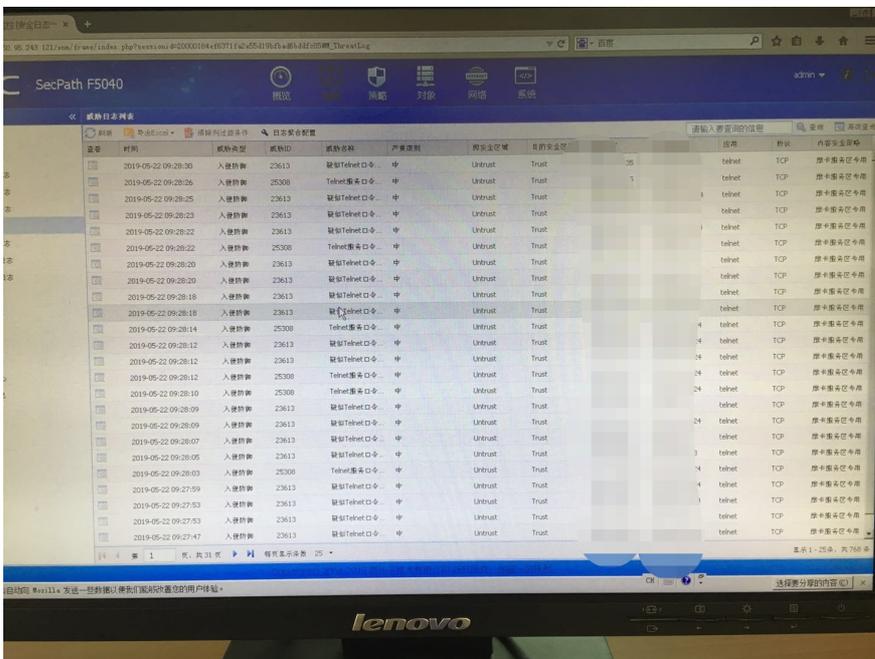
安全策略配置

名称	源安全域	目的安全域	类型	ID	描述	源地址	目的地址	服务	用户	条件	内容安全	安全引擎	流量	策略
堡垒机	Untrust	Trust	IPV4	8	堡垒机	所有	所有	所有	所有	允许	IPS: default AV: default	227847	66.36MB	<input checked="" type="checkbox"/>
允许访...	Untrust	Trust	IPV4	7	允许访RETS前置R ETS前置网非FTP重	所有	ftp	ping	所有	允许	IPS: default AV: default	0	0.00B	<input checked="" type="checkbox"/>
允许升...	Untrust	Trust	IPV4	4	所有	允许升通445	445端口	445端口	所有	允许	IPS: default AV: default	3.67*10 ⁶	746.73MB	<input checked="" type="checkbox"/>
允许3389	Untrust	Trust	IPV4	2	视各网网段	服务器段	TCP:3389	TCP:3389	所有	允许	IPS: default AV: default	10962	1.29MB	<input checked="" type="checkbox"/>
禁止338...	Untrust	Trust	IPV4	5	所有	所有	TCP:3389	445端口	所有	拒绝	IPS: default AV: default	33	2.21KB	<input checked="" type="checkbox"/>
禁止访...	Untrust	Trust	IPV4	6	所有	ETS前置网非FTP重	ftp	ping	所有	拒绝	IPS: default AV: default	0	0.00B	<input checked="" type="checkbox"/>
摩卡服...	Untrust	Trust	IPV4	9	摩卡服务器	所有	所有	所有	所有	允许	IPS: 摩卡库 AV: default	1.10*10 ⁷	1.70MB	<input checked="" type="checkbox"/>
病毒防护	Untrust	Trust	IPV4	1	所有	所有	所有	所有	所有	允许	IPS: default AV: default	1.92*10 ⁸	757.59KB	<input checked="" type="checkbox"/>
any to any	Local	Local	Trust	Trust	IPV4	0	所有	所有	所有	允许	IPS: default AV: default	6.54*10 ⁸	472.33KB	<input checked="" type="checkbox"/>

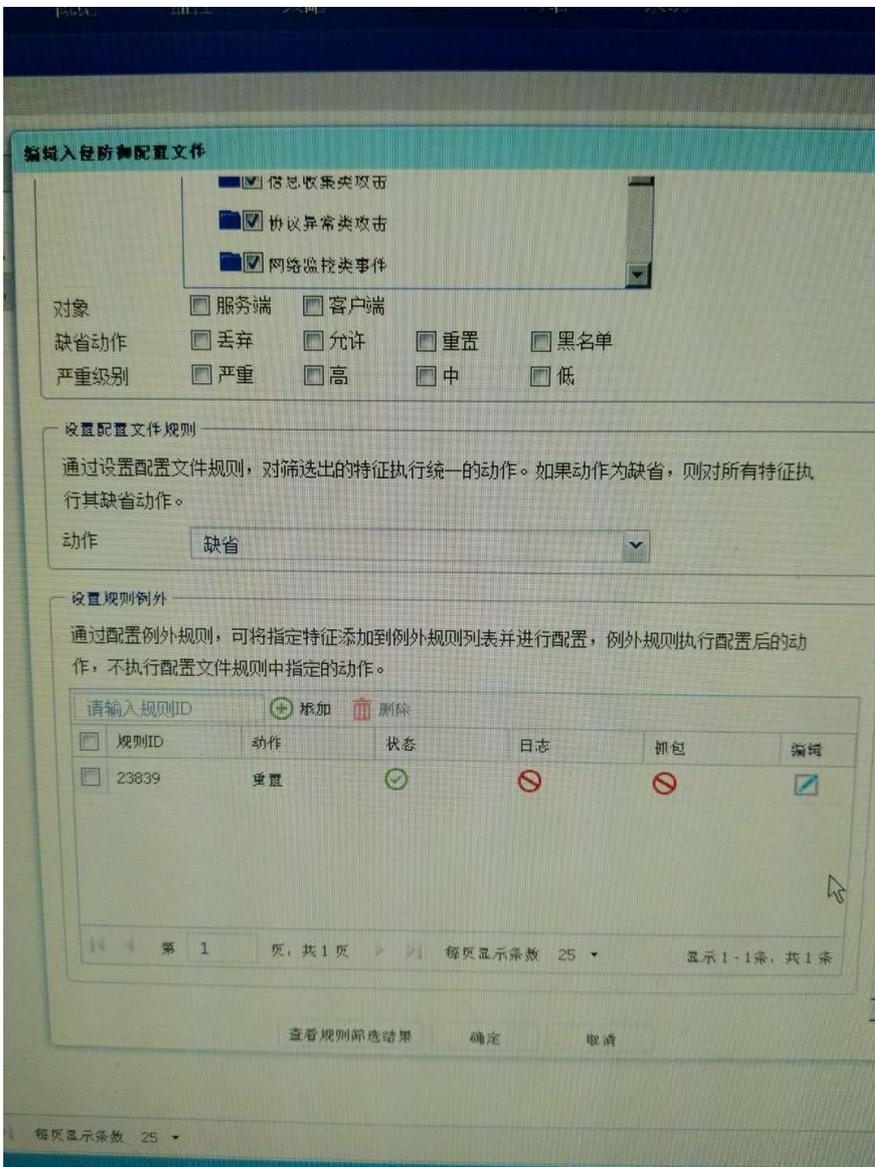
PS规则配置：例外规则ID23613和25308是禁止日志的，但是威胁日志还是能匹配上23613和25308



安全威胁日志



下面是客户最近添加的也是一样的问题



查看	时间	威胁类型	威胁ID	威胁名称	严重级别	源安全区域	目的安全区域	应用	协议	内容安全策略
	2019-05-27 16:22:34	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 16:22:32	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 16:19:00	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 16:18:58	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 16:17:12	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 16:17:10	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 16:11:56	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 16:11:54	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 15:36:19	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 15:36:18	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 15:22:58	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用
	2019-05-27 15:22:56	入侵检测	23839	Microsoft_Wind...	中	Untrust	Trust	microsoft-ds	TCP	威胁设备专用

过程分析

查看配置没有问题，最后找到研发分析，发现目前日志读取有如下限制：

目前版本IPS例外规则关闭日志只是不往info-center写了，还是往top写的。web上显示的日志是从ntp读的，将来会有版本支持关闭往top写日志。

解决方法

需要后续版本解决